METHOD AND SYSTEM FOR AUTHENTICATION THROUGH A COMMUNICATIONS PIPE

Field of Invention

The present invention relates to a data processing method for end user authentication over a network for purposes of obtaining secure functions or data from one or more remote computer systems. More particularly, the invention relates to a method of authenticating an end user to multiple remote computer systems using a communications pipe and a personal security device.

Background of Invention

One of the simplest and most commonly used authentication methods employed is the static password, whereby a client computer challenges an end user for a pre-determined password. Once the end user provides the correct password, access is permitted to secure functions or data available on one or more remote computer systems. A significant limitation of the current art is that localized authentication transactions are potentially vulnerable to compromise by unauthorized programs running on the local client or by other illicit means intending to monitor the password authentication process. In a single point authentication process, once a point of entry to a network is compromised, all locations using the same security codes are generally compromised as well.

One security method commonly used to overcome single point authentication failures employs the use of separate static passwords for each pre-determined secure resource. While this method is an improvement over a single multi-use password, this method is still vulnerable to illicit password monitoring, requires an end user to remember multiple passwords, and inefficiently ties up network resources by repeating the entire authentication process each time access to a different secure resource is requested.

Also, as a practical consideration, requiring an end user to remember several different passwords typically results in the same password being used for all secure resources, hence defeating the entire purpose of performing multiple authentications using static passwords.

A more sophisticated approach than the previously described methods, involves the use of personal security devices (PSD) such as smart cards, which allows storage of multiple credentials, passwords, certificates, private keys, etc. By implementing the use of smart cards, the ability to compromise passwords is significantly reduced. However, PSDs are still somewhat vulnerable to illicit monitoring during local client cryptographic key generation as described in the background of the invention section of cross-

referenced patent application, _____ OCL-1, "Method and System for Establishing a Remote Connection To a Personal Security Device." An additional limitation of this method becomes apparent when attempting to perform multiple authenticating transactions using a single PSD over a network connection. The PSD, beings a slow serial device, only allows one transaction to occur at a time. In addition, network contention and processor execution speed issues become particularly problematic when low bandwidth connections (e.g. dialup connections) are made between a client and a remote computer system during authentication with the PSD.

Summary of Invention

This invention resides in a method of authenticating an end user to one or more remote computer systems using a communications pipe to send authentication codes from a PSD to one or more secure remote computer systems. The remote computer system establishing and maintaining the communications pipe with the PSD performs an initial authentication, then acts as a secure hub and client authentication proxy for other remote computer systems requesting client authentication. In a multi-tasking operating environment, multiple authentications occur as background transactions, which are transparent to the end user. The remote computer system acting as a secure hub may form multiple communications pipes with other clients connected to a network.

In order to perform authentications, a communications pipe is established between a remote computer system and a PSD as previously described in cross-referenced patent application, _____ OCL-1, "Method and System for Establishing a Remote Connection To a Personal Security Device." A remote computer system requiring client authentication sends an authentication challenge to either the client and is redirected to the remote computer system acting as a secure hub or using a pre-established address, sends an authentication challenge directly to the remote computer system maintaining the communications pipe.

In a one embodiment of this invention, the remote computer system assigned as a secure hub performs the initial client authentication then routes subsequent authentication challenges through the communications pipe to the PSD for processing within the secure domain of the PSD, then returns the PSD generated authentication code back through the communications pipe over a network and to the challenging remote computer system.

In a second embodiment of this invention, the remote computer system established as a secure hub performs the initial client authentication then copies, if not already present, the PSD's authentication credentials through the communications pipe to a secure storage location within the secure hub. The secure hub using the transferred

PSD credentials and equivalent algorithms authenticates the client to subsequent remote computer systems by emulating the PSD.

In both embodiments of this invention, communications between local clients and remote computers systems over one or more networks should employ secure communications protocols as is described in the cross-referenced patent application, ___ OCL-1, which further reduces the likelihood of unauthorized access or interception. For non-proprietary transactions with the PSD, secure communications are optional.

There are several advantages to this invention when used in conjunction with the communications pipe. First and most importantly, authentication transactions are only performed in highly secure and protected domains, which greatly reduces the chances of unauthorized access or interception. Secondly, authentication transactions will occur more rapidly and seamlessly, since remote computer systems are generally provided with greater network bandwidth and processing power than local clients.

Lastly, by relocating the authentication process to a remote computer system, a more simplified means to perform end-to-end authentication and maintain an audit trail of transactions by authenticated end users and transactions with other remote computer systems is readily accomplished since all authentication transactions are routed through a remote computer system designated as a secure hub.

Additional security improvements may be facilitated by incorporating the use of hardware security modules (HSM) at designated remote computer systems implementing the secure hub portion of the invention. End-to-end security is enhanced since authentications and related transactions occur within the highly secure domains of a PSD and HSM.

Brief Description of Drawings

FIG. 1 - is a general system block diagram for implementing present invention.

FIG. 2 - is a detailed block diagram illustrating initial authentication challenge.

FIG. 3 - is a detailed block diagram illustrating initial authentication.

FIG. 4 - is a detailed block diagram illustrating remote authentication challenge.

FIG. 5 - is a detailed block diagram illustrating remote authentication.

FIG. 6 - is a detailed block diagram illustrating authentication credential transfer.

FIG. 7 - is a detailed block diagram illustrating remote authentication challenge (Alternate inventive embodiment.)

FIG. 8 - is a detailed block diagram illustrating remote authentication (Alternate inventive embodiment.)

Detailed Description of Preferred Embodiment

The steps involved in performing authentication through a communications pipe are shown in Figures 1 through 8. Figure 1 is a generalized system block diagram. Figures 2 through 5 illustrate one embodiment of the invention where responses to authentication challenges are generated within the secure domain of a Personal Security Device. Figures 6 through 8 illustrate a second embodiment of the invention where a remote computer system established as a secure hub provides the proper response to authentication challenges, rather than directing challenges through the communications pipe into the PSD for processing. Characters shown with a prime sign (e.g. C') indicate a duplicate of an original authentication credential. Other drawing details shown but not described in this application refer to information described in cross-referenced patent application, ___ OCL-1, "Method and System for Establishing a Remote Connection to a Personal Security Device."

Referring now to FIG. 1, a generalized system block diagram of the invention where Client 10 and a connected Personal Security Device 40 is connected over a network 45 with a remote computer system 50 using a communications pipe 75 as described in co-pending patent application _____ OCL-1. A remote computer system 50, is operating as a secure hub following initial authentication as described below, to service authentication requests made by other remote computer systems sent over a network 45 or 45A.

The remote computer system 150 is an example of a system requiring authentication when a request for secure functions or data is sent from client computer 10 over the networks 45 and 45A. The communications pipe 75 applies to authentication transactions but does not restrict nor control non-secure transactions occurring over either network 45 or 45A.

Networks 45 and 45A may be a common network as in a virtual private networking arrangement or separate networks such as private intranet and public internet arrangements. The networks 45 and 45A are depicted separately for illustrative purposes only. No limitation is intended in the number of PSDs and clients forming communications pipes 75 with one or more secure hubs 50; nor should any limitation on the number of remote computer systems 70 available for authentication be construed from the drawing. Transactions not involving authentications are not restricted to the secure hub.

The basic operation of the secure hub may be initiated when an end user at a client requests access to secure functions or data contained on one or more remote computer systems connected by a network. An available remote computer system, in which a communications pipe has been established as described in co-pending application OCL-1, authenticates the end user and client using the security mechanisms contained within the secure domain of the PSD. Alternatively, an external event such as a need to update information within a PSD may trigger a remote computer system other than the secure hub to initiate the authentication process.

Once an initial client authentication has been accomplished by the remote computer system, subsequent authentication challenges transmitted over a network 45 or 45A made by other remote computer systems are directed to the remote computer system 50 acting as a secure hub and depending on which embodiment of the invention employed, are either routed through the appropriate communications pipe 75 to PSD 40 or are directly authenticated by the remote computer system 50.

Referring to FIG. 2, to establish a secure hub, a Client 10 causes an authentication challenge to be generated on a remote computer system 50, by requesting access to secure functions or data over a network 45 or 45'. Upon receiving the request from client 10, remote computer system 50 generates an authentication challenge 205 within a secure domain designated as authentication routine 65. The authentication challenge is processed by an API level program 100 and routed 200 to an APDU interface 55 for translation into an APDU format. The APDUs are then sent 220 to a Security Module 225 for encryption. The encrypted APDUs are then routed 230 to a Pipe Server 70 for encapsulation into outgoing messaging and sent 210 to the communications programs 105 for transmission over the communications pipe 75, through the network 45 into the network interface 130 of the client 10. The incoming messages are then routed 240 to communications programs 105 for processing.

Following processing, the messages are sent 250 to a pipe client 15 for separation of the encapsulated APDUs. The APDUs are then sent 260 through a hardware device port 5 assigned to a PSD Interface 25. PSD Interface 25 routes the incoming APDUs into the PSD 40 via connection 30, where it is subsequently decrypted and processed within its secure domain 35.

Referring to FIG. 3, once PSD 40 has processed the authentication challenge within the secure domain of the PSD 35, an authentication response message is generated using a pre-established cryptography method.

The authentication response is sent in APDU format from PSD 40 through connection 30 and into PSD interface 25. The PSD secure response is then routed 370

through hardware device port 5 and sent 360 to the Pipe Client 15 for processing and encapsulation. The resulting message packets are then sent 350 to the Client-side Communications Programs 105 for processing, encryption using a pre-established secure communications protocol and incorporation into outgoing message packets 340. The message packets 340 containing the encapsulated APDUs are transmitted 75 over the network 45 via a network interface card (I/O) 130.

The Remote Computer System 50, receives the message packets 335 containing the encapsulated APDUs from the network 45 via a network interface card (I/O) 130 installed on the Remote Computer System. The incoming messages are processed and decrypted using the pre-established cryptography method employed in the secure communications protocol by the server-side Communications Programs 105 and routed 310 into the Pipe Server 70 for secure APDU extraction. The extracted secure APDUs are sent 330 to the Security Module 325 for decryption of the secure APDUs using the pre-established cryptography method. The decrypted APDUs are then routed to the APDU Interface 55 for processing and translation into a higher-level format and sent 300 to API Level programs 100 for processing. If authentication is successful, the remote computer system 50 allows access to secure functions or data and establishes itself as a secure hub. If authentication fails, the end user will be unable to access secure functions or data.

Referring to FIG. 4, once the secure hub has been established as previously described, remote authentication of additional remote computer systems may be accomplished. Remote authentication may be initiated either by a client's request for access to secure functions or data or by other remote computer systems to perform transactions within the secure domain of a PSD.

To perform a remote authentication, a challenge 85 is issued by a second remote computer system 150. The challenge is routed over a network 45, into the secure hub 50. The incoming challenge is processed and decrypted in the secure hub 50 using the pre-established cryptography method employed in the secure communications protocol by the server-side Communications Programs 105 and routed 85 to an API level program 100 where it is processed and routed 400 to an APDU interface 55 for translation into an APDU format. The APDUs are then sent 420 to a Security Module 425 for encryption. The encrypted APDUs are then routed 430 to a Pipe Server 70 for encapsulation into outgoing messaging and sent 410 to the communications programs 105 for transmission over the communications pipe 75, through the network 45 into the network interface 130 of the client 10.

The incoming messages are then routed 440 to a communications programs 105 for processing. Following processing, the messages are sent 450 to a pipe client 15 for separation of the encapsulated APDUs. The APSUs are then sent 460 through a hardware device port 5 assigned to a PSD Interface 25. PSD Interface 25 routes the incoming APDUs into the PSD 40 via connection 30, where it is subsequently decrypted and processed within its secure domain 35.

Referring to FIG. 5, once PSD 40 has processed the authentication challenge within the secure domain of the PSD 35, an authentication response message is generated using a pre-established cryptography method. The authentication response is sent in APDU format from PSD 40 through connection 30 and into PSD interface 25. The PSD secure response is then routed 570 through hardware device port 5 and sent 560 to the Pipe Client 15 for processing and encapsulation. The resulting message packets are then sent 550 to the Client-side Communications Programs 105 for processing, encryption using a pre-established secure communications protocol and incorporation into outgoing message packets 540. The message packets 540 containing the encapsulated APDUs are transmitted 75 over the network 45 via network interface card (I/O) 130.

The Remote Computer System 50, receives the message packets 535 containing the encapsulated APDUs from the network 45 via network interface card (I/O) 130 installed on the Remote Computer System. The incoming messages are processed and decrypted using the pre-established cryptography method employed in the secure communications protocol by the server-side Communications Programs 105 and routed 510 into the Pipe Server 70 for secure APDU extraction. The extracted secure APDUs are sent 530 to the Security Module 525 for decryption of the secure APDUs using the pre-established cryptography method. The decrypted APDUs are then routed 520 to the APDU Interface 55 for processing and translation into a higher-level format and sent 500 to API Level programs 100 for processing. Authentication Module 65 within the secure hub remains inactive during the transfer of authentication information. The authentication response message is then routed 85 into the Communications Programs 105 where the response is sent over the network 45 in a pre-established secure communications protocol to the challenging remote computer system 150.

The incoming response message is decrypted and sent to an Authentication Module 95. If authentication is successful, the remote computer system 150 allows access to secure functions or data. If authentication fails, the end user will be unable to access secure functions or data.

Referring to FIG. 6 depicts an alternate embodiment of the current invention where the remote computer system 50 established as a secure hub transfers copies of the PSD 40 credentials C 35, if not pre-existing on the secure hub. To perform credential transfer, an initial authentication transaction is performed by a remote computer system 50 as previously described. Following authentication, additional commands are sent by the remote computer system 50 to transfer the specified credentials.

The credentials are generated using a pre-established cryptography method and sent in APDU format from PSD 40 through connection 30 and into PSD interface 25. The PSD secure response is then routed 670 through hardware device port 5 and sent 660 to the Pipe Client 15 for processing and encapsulation. The resulting message packets are then sent 650 to the Client-side Communications Programs 105 for processing, encryption using a pre-established secure communications protocol and incorporation into outgoing message packets 640. The message packets 640 containing the encapsulated APDUs are transmitted 75 over the network 45 via a network interface card (I/O) 130.

The Remote Computer System 50, receives the message packets 635 containing the encapsulated APDUs from the network 45 via network interface card (I/O) 130 installed on the Remote Computer System.

The incoming messages are processed and decrypted using the pre-established cryptography method employed in the secure communications protocol by the server-side Communications Programs 105 and routed 610 into the Pipe Server 70 for secure APDU extraction. The extracted secure APDUs are sent 630 to the Security Module 625 for decryption of the secure APDUs using the pre-established cryptography method. The decrypted APDUs are then routed 620 to the APDU Interface 55 for processing and translation into a higher-level format and sent 600 to API Level programs 100 for processing and subsequently sent 605 to the Authentication Module 65 for secure storage and future use. The transferred authentication information is shown in FIG. 6 as C'.

In FIG. 7, an authentication challenge 85 is sent by a remote computer system 150 over a network 45. Remote Computer System 50 receives the incoming challenge 85 from the network 45 via network interface card 130 installed on the Remote Computer System. The incoming challenges 85 are processed and decrypted using the pre-established cryptography method employed in the secure communications protocol by the server-side Communications Programs 105 and routed to API Level programs 100 for processing. The processed challenge is then sent 705 to the Authentication Module 65

for authentication using the PSD's 10 transferred credentials C' 35'. The communications pipe 75 may remain intact during this process to allow for other transactions to occur.

Referring to FIG. 8, the secure hub 50 generates an authentication reply within the Authentication Module 65 which is sent 805 to the API Level Programs 100 for processing, and subsequently routed 810 to the Server-side Communications Programs 105 for processing, encryption using a pre-established secure communications protocol and incorporation into outgoing message packets. The message packets are routed over the network 45 to the challenging remote computer system 150. The incoming messages are then decrypted and the authentication reply processed by an internal authentication module 95. If authentication is successful, the remote computer system 150 allows access to secure functions or data. If authentication fails, the end user will be unable to access secure functions or data.

The foregoing described embodiments of the invention are provided as illustrations and descriptions. They are not intended to limit the invention to precise form described. In particular, it is contemplated that functional implementation of the invention described herein may be implemented equivalently in hardware, software, firmware, and/or other available functional components or building blocks. Other variations and embodiments are possible in light of above teachings, and it is not intended that this Detailed Description limit the scope of invention, but rather by the Claims following herein.